Docket No.: 10013499-1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Joubert Berger et al.

Application No.: 09/896,385

Confirmation No.: 9535

Filed: June 29, 2001

Art Unit: 2127

For: SYSTEM AND METHOD FOR MANAGEMENT OF COMPARTMENTS IN A TRUSTED OPERATING SYSTEM

Examiner: Kenneth Tang

DECLARATION OF JOUBERT BERGER SUBMITTED UNDER 37 C.F.R. 1.131

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

1. My name is Joubert Berger, I am over 21 years of age, and make this declaration based upon my own personal knowledge.

2. I am one of the inventors of the invention claimed in the above-identified patent application.

3. Prior to June 1, 2001, I conceived the idea of a system and method for management of compartments in a trusted operating system as recited at least in the pending claim 10 of the above-identified patent application. Accordingly, prior to June 1, 2001, I disclosed my invention to my then employer, Hewlett Packard Company.

4. Attached hereto as Exhibit A is a copy of a Functional Specification that I prepared prior to June 1, 2001. This Functional Specification establishes my conception of at least one embodiment of the subject matter claimed at least by pending claim 10 of the above-identified patent application prior to June 1, 2001.

5. Attached hereto as Exhibit B is a copy of an invention disclosure form that I submitted to Hewlett-Packard Company prior to June 1, 2001, for the filing of a patent application. Hewlett-Packard Company considered the invention disclosure that I submitted and approved the filing of a corresponding patent application. The application was filed with the USPTO on June 29, 2001.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Date: 1/7/2005

Joubert Berger
(Joubert Berger)

Functional Specification

Title:	Trusted Linux Compartment Management Utilities
Author:	Joubert Berger

HP CONFIDENTIAL

REDACTED

Exhibit A - 26 pages

1 - Contents

REDACTED

REDACTED

REDACTED

REDACTED

3 – Introduction

3.1 Abstract

In order to manage a trusted system, a number of utilities are needed to help manage the compartments. This paper identifies the immediate utilities needed for the Trusted Linux OS.

REDACTED

REDACTED

5 – Specific Feature Requirements

5.1 Overview of Feature 1 (Compartment Creation/Modification)

In order to allow applications to run in different compartments, they must be installed in chrooted environments. Additionally, because compartments are represented internally as integers and it is difficult to remember all the different numbers representing compartments, a mapping database must be created that allows one to map the compartment numbers to compartment names. All these functions fall under the category of compartment creation/modification. A command line utility must be created that allows a user to manipulate all the operations of creating a compartment.

5.1.1 Operational Description

This utility will be used in a number of ways:

- Create a compartment
- Create a chrooted environment
- Modify a compartment name
- Delete a compartment name

5.1.2 Add

When creating a compartment, the user must never be aware about how the compartment representation is implemented (i.e. an integer). The user will only know about compartment symbolic names. Therefore, when the user creates a compartment he will be registering the compartment name with the Trusted Linux OS. The utility will assign an integer number to this compartment name, which is the integer that represents the compartment inside the kernel.

REDACTED

5.1.2.9 Examples

```
tlcompadd <compartment name>
tlcompadd web
tlcompadd mail
```

REDACTED

REDACTED

5.1.4 Rename

When modifying a compartment name you are just renaming the compartment name to something new. For example, modifying the compartment name *mail* to *mailserver*

REDACTED

5.1.4.9 Examples

```
tlcompren <old compartment name> <new compartment name>
tlcompren web webserver
tlcompren mail qmail
```

5.1.5 Remove

When deleting a compartment, the compartment name is removed from the database and kernel. Additionally, the chrooted environment can be removed if the –r option is given. A users must first confirm that he wants to remove the compartment. If the –f option is given, then the confirmation of removing the compartment is not performed.

REDACTED

5.1.5.9 Examples

```
tlcomprm –f <compartment name>
tlcomprm –f web
tlcomprm mail
```

The –f option means not to confirm the deletion of the chrooted environment.

REDACTED

REDACTED

REDACTED

5.2 Overview of Feature 2 (Get Compartment Name)

While working in a compartment, it is sometimes advantages to know what compartment one is in. A command must be provided that will display the current compartment.

5.2.1 Operational Description

A command is execute that will display the symbolic name of the compartment.

5.2.2 Functionality

When you execute the command, the current compartment name is displayed.

REDACTED

5.2.2.9 Examples

tlgetcomp

This should return the symbolic name of the compartment.

REDACTED

5.3 Overview of Feature 3 (Set Compartment Name)

A tool that is needed when integrating applications on a system is a tool that allows one to change from one compartment to another. This capability allows us to integrate applications easy because we can change compartments real quick. Additionally, this tool needs to be able to run a command in a compartment. This allows us to create tools that allow us to run commands in a particular compartment.

5.3.1 Operational Description

A command is execute with the compartment name at a parameter. A new shell i started running in the new compartment. An option is provided, where one can run a command instead of starting a shell. Note that this command will not run the startup scripts in the compartment.

5.3.2 Functionality

Execute the command to change the compartment that the user is in. When the user executes this new command, a new shell is started in the new compartment.

REDACTED

5.3.2.9 Examples

```
tlsetcomp <compartment name> -c <command name>
ltsetcomp web
tlsetcomp web –c /usr/bin/httpd
```

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

ritc in Dark Ink on Front Side Only, P se

IWW

INVENTION DISCLOSURE

PDNO 3499 DATE RCVD

PAGE ONE OF ___

ATTORNEY LJG/ISD-AT

Descriptive Title of Invention: Compartment Management fa Trusted Linux Compartments

Name of Project:

Product Name or Number:

Was the invention described in a lab book or other record? If so, please identify (lab book #, etc.)

yes, functional Spec "Containment Utilities Functional Spec" by Joubert Berger

Signature of Inventor(s): Pursuant to my (our) employment agreement, I (we) submit this disclosure on this date: [ ].

	Joubert Berger	Joubert Berger			
Employee No.	Name	Signature	Telnet	Mailstop	Entity & Lab Name
	Scott Leerssen				
Employee No.	Name	Signature	Telnet	Mailstop	Entity & Lab Name
Employee No.	Name	Signature	Telnet	Mailstop	Entity & Lab Name
Employee No.	Name	Signature	Telnet	Mailstop	Entity & Lab Name

(If more than four inventors, include additional information on another copy of this form and attach to this document)

REDACTED

Exhibit B – 3 pages

REDACTED

W :in Dark Ink on Front Side Only, Ple

Description of Invention:

A. Description of the construction and operation

In order to manage the compartments in a Trusted Linux, utilities are needed to help ~~manage~~ manipulate these compartment. These utilities are needed to create compartments delete compartments, and rename compartments. Another important ~~to~~ utility is to start the compartment. All these tools will ease the managing of a ~~Trusted~~ Trusted Linux system.

B. Advantages over what has been done before.

There are no such utilities sine this type of containment does not exist. The advantage is that it simplifies how to administrate compartments on a trusted OS.

C. Problems solved

By having these utilities, the manipulation of compartment becomes very easy. One does not have to use cryptic commands because our utilities simplifies this.

D. Prior solutions and their disadvantages (if available, attach copies of product literature, technical articles, patents, etc.).

REDACTED